PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06K 19/067

A1

(11) International Publication Number: WO 00/31685

(43) International Publication Date: 2 June 2000 (02.06.00)

(21) International Application Number: PCT/AU99/01037

(22) International Filing Date: 22 November 1999 (22.11.99)

(30) Priority Data:

PP 7248	20 November 1998 (20.11.98)	AU
9927002.7	15 November 1999 (15.11.99)	GB

(71) Applicant *(for all designated States except US)*: KEYCORP LIMITED [AU/AU]; Level 9, 67 Albert Avenue, Chatswood, NSW 2067 (AU).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: WOOD, John [AU/AU]; Lot 50, Sturdee Lane, Lovett Bay, NSW 2105 (AU). McKEON, Brian [AU/AU]; 24 Holdsworth Avenue, St. Leonards, NSW 2065 (AU). HOCHFIELD, Barry [GB/GB]; 21 Dalserf Crescent, Giffnock, Glasgow G46 6ZB (GB).

(74) Agent: WATERMARK PATENT & TRADEMARK ATTORNEYS; Unit 1, The Village, Riverside Corporate Park, 39–117 Delhi Road, North Ryde, NSW 2113 (AU).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

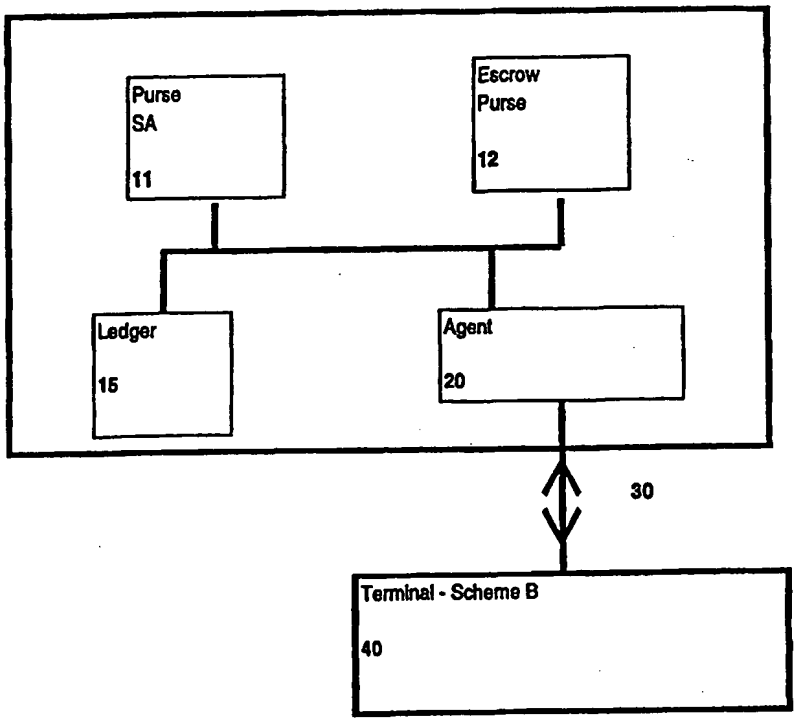
Published

With international search report.

(54) Title: MULTIPLE SCHEME ELECTRONIC CASH SYSTEM

(57) Abstract

Disclosed is an improved arrangement for electronic cash transactions using smartcards. A smartcard is provided with an additional memory for electronic cash, which is not accessible to the user. When certain types of transactions are performed – for example, a transaction according to a different electronic cash scheme, or for a particular off–line party – the main card purse is debited, and the additional memory credited. Thus, a more secure and flexible off–line transaction can be effected.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

MULTIPLE SCHEME ELECTRONIC CASH SYSTEM

Technical Field

The present invention relates to smart cards, and in particular, to smart cards which, either solely or in conjunction with other purposes, are used to provide electronic cash services.

Background Art

Schemes have been proposed by which customers could use a smart card - that is, a card incorporating a microprocessor - to effect a transaction which has been traditionally undertaken by cash. Often, these are low value transactions where use of credit card or debit card type facilities is not convenient, particularly from the perspective of the vendor. Such applications may be, for example, newspapers, fast food outlets, public transport tickets, telephone services and numerous other applications.

Various schemes have been proposed and trialled in relation to such electronic cash systems. Generally, the schemes involve a certain verified amount of electronic cash being deposited on the card, this cash being guaranteed by the scheme in some manner. Encryption schemes are used to ensure that the user can not fraudulently add extra value to the electronic purse. Examples of such schemes are Mondex™, Chipper ™ and Proton™.

One aspect of the various competing schemes proposed or in use is that in general they are not interoperable. They use different encryption schemes and operating protocols, such that a terminal configured for one scheme will not be able to accept additional schemes, unless it is also configured to accept such additional schemes. The terminals for most such schemes require a specific integrated circuit, known as a Secure Access Module (SAM) to be provided. The more SAMs that are required to be added to a terminal, the greater the cost of the terminal. One of the specific objectives of the electronic cash systems is to make the terminals inexpensive, so that they will be widely used by merchants. However, if each merchant is required to have a terminal supporting many different schemes, due to a proliferation of such schemes in the community, and in order to do this each terminal must have multiple SAMs then the cost of the terminals will inevitably be higher.

In certain applications, it is difficult to go "on-line" to a payment network at the time of the service purchase. However, it is highly desirable that electronic cash schemes operate in such environments, or they will be at a practical disadvantage to physical currency.

Take for example, "pay as you talk" class debit mobile phone service provision, such as is available in the United Kingdom. The most popular method of payment at present is to purchase paper "scratch cards" which contain "one time top up" authentication codes. These codes are entered into a telephone handset via a keypad and then can be transmitted to a central server where a "meter/tariff" account resides either on the handset or all on a central server that controls the access times for each particular handset.

A key disadvantage with scratch cards is the cost of distribution, which represents a significant percentage of the telecom operator's gross revenue (typically – 15% - 20%). For mobile phone network operators this can run into many millions of pounds per year.

Mobile handsets with a smartcard interface (slot) specifically to communicate with card based applications that can perform the authentication "top up" function and provide payment are known. The method for payment in such an arrangement is for the handset to "go on-line" and transfer funds either by authorising a credit or debit transaction from a cardholder's bank account to the telecom network operator directly, or to transfer funds directly in the case of e-cash from a handset connected smartcard to a central server.

Consider the Mondex™ E-cash scheme. As all Mondex™ value transfers must occur between two Mondex™ Purse software applications, using Mondex™ for e-payment over mobile phone networks such as GSM, requires a suitable data channel. In the case of GSM the only such data channel available (without adding more expensive modem adaptation circuits to each handset) is GSM's Short Messaging Service (SMS). SMS is very low bandwidth and is "non-isochronous packet network like" in behavior. This gives very poor performance for a point to point transaction such as a Mondex™ transfer resulting in long transaction times and unreliability.

A further problem is the cost associated with revenue collection, fro example from parking meters or the like. A suitable electronic cash system would in principle reduce the problems of coin collection and vandalism, but only if a simple, reliable scheme can be implemented.

It is an object of the present invention to provide an arrangement whereby terminals supporting only one scheme can be used by smart card holders who subscribe to another scheme.

It is a further object of the present invention to provide a mechanism for effecting deferred payment, particularly for small value transactions, in a smartcard based system.

Summary of Invention

Broadly, the present invention envisages providing, in addition to the single purse in a conventional smart card, an additional, escrow purse denominated in that scheme, with a software agent provided on the smart card. The agent is enabled to communicate with a terminal operating on a different electronic cash scheme, to transfer electronic cash according to that scheme, and to meanwhile debit the main purse of the card scheme and credit the separate escrow purse within the smart card. Thus, the electronic funds are removed from the funds available on the smart card to the holder. The funds in the additional purse are marked and recorded, preferably via some ledger facility, as being transferred to the alternative scheme to the credit of the particular merchant. When the smart card is later inserted into a more sophisticated terminal, the balance in the additional or escrow purse is reconciled, so that the funds can be transferred via the merchant's scheme to the merchant. More than one such escrow purse may be provided, to allow for separate escrow purses relating to different electronic cash schemes, or possibly currencies.

The advantage of such a scheme is that the agent can be implemented purely in software within the smart card. The merchant's terminal needs only to support one of the schemes with which the agent is configured to operate, thereby reducing the cost of the merchant terminal. It is inherent in such a system that there needs to be a high degree of trust in the agent as it is mediating between schemes operating on different encryption techniques. Each of these schemes operates independently and does not necessarily fully trust the other. Accordingly, the arrangement proposed is particularly applicable to relatively low value electronic cash transfers, where the amounts involved do not constitute significant loss if the transaction is not completed for some reason. Daily amount and total amount limits on the escrow purse are desirably implemented to minimise the risk associated with fraud or misuse.

According to another aspect, the escrow purse is used to accumulate funds in off-line transactions, even where the same scheme is used by a terminal. This is particularly applicable to situations where it is difficult or expensive to provide a fully functioned terminal. Ledgers and reconciliation occur as in the multi-scheme implementation. Preferably, both multi-scheme and accumulation approaches can be used in tandem.

Whilst the advantages of the inventive arrangement are most clear where a relatively low cost merchant terminal is used, it will be apparent that this arrangement could be used with more sophisticated terminals - for

example, ATM type devices. Where on-line connections are available, from the terminal, the transaction could be affected directly via the respective schemes and/or issuers. However, the present invention has greater advantages in the off-line situation, as it allows for the smart card to still reflect the correct value of available electronic cash in the customer - accessible purse, and to have an amount for later reconciliation stored in the escrow purse, which is not susceptible to variation or alteration by the card user. We have accordingly applied the term escrow - that is, the funds are held in this purse, pending later reconciliation, and are not available to the card holder for use in subsequent purchases.

Accordingly, the present invention allows the transaction to be conducted without the terminal or card operator being concerned with or even aware of which scheme is being used. The cardholder loads the smartcard with a value under either a principal or selected scheme, and is thereafter not required to draw distinctions. In some schemes, if the scheme requires different or additional information or interactions, then the usual prompts will guide the user.

The present invention is also applicable to other devices which function in similar ways to a smartcard – for example, devices which have been used to provide utility and other services – and these are intended to be encompassed by the broad term smartcard in this specification. The devices may use contact or contactless interfaces.

Brief Description of Drawings

The present invention will be further described with reference to the accompanying figures, in which:

Figure 1 is a block diagram of the schematic operation of the smart card in communicating with a simple terminal;

Figure 2 is a schematic illustration of the operation of the inventive smart card with a more sophisticated terminal;

Figure 3 is a schematic illustration of the functional blocks within the smart card where the agent has multiple scheme functionality;

Figure 4 illustrates schematically the operation of one aspect of the invention.

Detailed Description

The present invention will be described in relation to a smart card, which is envisaged as having only electronic purse type functionality. Whilst this may be the case, it is likely that other functionalities - for example, conventional financial services, identification or access functionality - may also

be included on the smart card. Only the aspect dealing with electronic cash will be discussed. The smart card may be of any conventional type, subject to sufficient non-volatile memory to support the application described. The application will be discussed in the context of what would be described as Schemes A, B, etc - it would be appreciated that these could be any electronic cash or similar schemes. For example, apart from the broad schemes previously discussed, they could include the ability to interoperate with specific schemes for telephone access or public transport.

With reference to figure 1, suppose a customer has a smart card, issued pursuant to Scheme A, and wishes to make a purchase from a merchant who has a terminal operable only under Scheme B. The smart card 10 is placed in communication with the terminal - this could be either via a non contact or contact technique - so as to establish communications link 30. After normal power-up procedures on the smart card, agent 20 determines that the terminal 40 operates under Scheme B, and then engages an appropriate interface. The purchase amount is advised, for example $10.00, from the terminal to agent 20. After the appropriate identification procedures and authorisation has occurred - for example, a PIN number has been provided by the genuine card holder - agent 20 commences to perform the transaction. Electronic cash equivalent to $10.00 is deleted from the balance of purse A, and is credited to the balance of the escrow purse 12, also operating under scheme A. Details of the merchant, date, terminal scheme, etc are stored in ledger 15, to enable later reconciliation. Agent 20 then advises the terminal of the transfer of an appropriate amount of electronic cash under Scheme B, such transfer to be completed once smart card 10 has been inserted into a terminal arrangement capable of reconciling the transaction. The merchants terminal 40 may optionally retain appropriate details of the card, user, amount and date for later checking against finalisation of the transaction. Low cost terminals dealing with low value transactions may not retain a log, and simply rely on the single log within the purchaser's card. Alternatively, the merchant's card may be used to retain such a log rather than the terminal. A flowchart illustrating this process for an off-line situation is shown as figure 5.

Figure 3 illustrates schematically the arrangement of the agent 20 within smart card 10. The control software 25, after the card is powered up, determines the scheme in which the terminal operates - for example, this may be scheme B. It then selects from the schemes available to it - shown as interfaces 21 to 24 - the correct application to provide an appropriate interface, in this case scheme B. This provides also the correct protocols for interacting

with a scheme B terminal, so that from the perspective of the terminal 40 it is interacting with a valid scheme B card. Each interface also communicates with a respective escrow purse 26, 28, 29 and 30, distinct for each scheme. Alternatively, a single escrow purse could be used with some indicia to associate the escrow purse with a particular scheme. The control 25 (or alternatively each interface 26, 28,29,30) debits the main purse operating under scheme A as appropriate for each transaction.

The card user has access only to the balance available in purse A, and optionally the ledger and escrow purse as read only values. The ledger 15 can only be rectified and reconciled once appropriate communications with the issuer, or at least a more sophisticated terminal supporting multiple schemes, occurs.

Figure 2 illustrates a situation when, at some later time after transactions have occurred off-line, smart card 10 is presented to a more sophisticated terminal 50. Figure 6 is a flowchart illustrating this process. Smart card 10 may well be inserted into terminal 50 for some other purpose than reconciliation - for example, obtaining an account balance. The terminal and smart card software interact using the details in the ledger and the escrow purse so as to reconcile the earlier off-line transaction, empty the escrow purse, and arrange transfer of the appropriate alternative scheme funds to the merchants.

In an alternative implementation, the smart card may retain a specific purse under the alternative schemes. In this implementation, the agent would mediate transfers amongst these purses, subject to the overall security arrangements for the principal or A scheme. It will be apparent that the agent needs to be placed in a secure memory within the smart card, so that it is not subject to alteration by parties other than the card issuer.

In a further application, a temporary escrow purse may be used to enable small value transactions i.e. several cents for a time period when operating a telephony device - to be added up, and the transaction finalised once the call is terminated. For example, the agent may be enabled to accept the 'click' protocol operating on the telephony service providers lines, so as to add up a progressive tally. At the end of the session, the proper amount could be debited from the A purse, and added to the appropriate escrow purse - for example, for one specific telecommunications provider or marked up to credit that provider through an alternative scheme.

It will be appreciated that the agent will simply select the appropriate scheme, based upon those present at the terminal. Initially, it would attempt

to utilise its principal scheme, and utilise others in some order of hierarchy. However, the arrangement is preferably such that the internal interfacing is transparent to the user - as far as the cardholder is concerned, all of these are occurring as scheme A type transactions and a consistent interface is presented to him by the smart card at each terminal to which it is inserted.

Referring to Figure 4 there is illustrated a smartcard, generally designated 10a.

Another aspect of the present invention provides a service provision including the steps of:

(a) presenting the smartcard 10a to at least one service access point 100a;

(b) undertaking mutual authentication of the smartcard 10a and the access point 100a, in a way known in the art;

(c) the access point 100a communicating a required tariff to the ledger 15a;

(d) the ledger 15a establishing whether sufficient funds are held in a card holder purse 11a;

(e) transferring funds from the user purse 11a to the escrow purse 12a, i.e. purchasing the service, optionally under user control;

(f) updating the ledger 15a by recordal of transfer of funds to the escrow purse 12a and service provider ID in the ledger 15a.

The improvement thus allows for payment to be "deferred".

This aspect is particularly relevant to pre-pay mobile phones, and funds collected later, under control of a "revenue collection body". The use of SMS' could, therefore, be greatly reduced by use of the improvement. The revenue collection body could use a server on the telecom network which "pulls" the funds from the escrow purse via the SMS, transparent to the card holder/phone user, or simply when the card holder/phone user connects the smartcard to the "revenue collection body" to access other services it provides. It is therefore envisaged that the "revenue collection" function, i.e. the emptying of the escrow purse, could be performed by the same bank that issued the payment smartcard.

Another application could be where card 10a based software application "Intf Module" (2a) , controlled by the "Ledger Agent application" (15a), authorises some other service provision point such as a ticket turnstile at a theatre, on a public transport vehicle or even a parking or utility meter.

This allows the service provision point to be completely "off-line" obviating the need and cost of networking. Again the revenue collection function would occur after the fact, and other "service token" reconciliation

functions could be included in the Intf Module (2a) application.

It would be apparent to the skilled worker that variations and additions are possible within the general inventive concept disclosed.

5

CLAIMS

1. A smartcard for conducting electronic cash transactions using one of a plurality of terminal devices, said smartcard including a main purse in secure memory for storage of data representing electronic cash, and means for interoperating with one of said terminals,

characterised in that said smartcard further includes an escrow purse, into which electronic cash can be placed under control of the smartcard, but cannot be subsequently used by the smartcard user.

2. A smartcard according to claim 1, wherein the smartcard further retains ledger information to allow for reconciliation of the funds in the escrow purse with the transactions undertaken.

3. A smartcard according to claim 2, wherein the reconciliation occurs when the smartcard is presented to an on-line terminal.

4. A smartcard according to claim 1, wherein the smartcard is enabled to operate on a first electronic cash scheme, and additionally on one or more additional schemes, and the escrow purse retains the value in said first scheme of electronic cash spent on said additional schemes.

5. A smartcard according to claim 4, wherein said smartcard includes a software agent adapted to provide electronic functionality with a terminal operating according to either said first or said additional electronic cash schemes.

6. A smartcard according to claim 5, wherein upon establishing communications with said terminal, said software agent determines an electronic cash scheme which is available for both the smartcard and the terminal, and communicates according to that scheme, without reference to the card user.

7. A smartcard according to claim 1, wherein the escrow purse is used to retain transactions in a different currency to the main purse.

8. A smartcard according to claim 1, wherein the escrow purse is used to retain incremental debits, for later consolidation and debiting.

9. A smartcard according to any one of the preceding claims, wherein the smartcard and terminal communicate using a wireless system.

10. A method for allowing a smartcard and terminal to conduct an electronic cash transaction, said smartcard having an application operating according to a first electronic cash scheme and said terminal having an application operating according to a second electronic cash scheme, said smartcard having a main purse in secure memory for storage of data representing electronic cash, an escrow purse purse in secure memory for storage of data representing electronic cash,
said method including the steps of
(a) establishing communications between the smartcard and the terminal;
(b) said smartcard determining which electronic cash scheme is supported by said terminal;
(c) said terminal, placing a request for transfer of electronic cash using said second scheme with said smartcard;
(d) said smartcard determining if the value of cash requested is available in the main purse, and only proceeding if the value is available;
(e) said smartcard debiting the value from the main purse, crediting the escrow purse, and transferring the value of electronic cash requested in said second scheme to said terminal;
such that said terminal receives electronic cash according to said second scheme, said main purse is debited according to said first scheme and a credit of the same value is placed in said escrow purse for later reconciliation.

11. A method for allowing a smartcard and terminal to conduct an electronic cash transaction, said smartcard having a main purse in secure memory for storage of data representing electronic cash, an escrow purse in secure memory for storage of data representing electronic cash, said terminal being enabled to communicate with said smartcard,
said method including the steps of:
(a) establishing communications between the smartcard and the terminal;
(b) establishing user authentication for debiting of funds;
(c) said terminal placing a request for transfer of electronic cash with said

smartcard;

(d) said smartcard crediting the value to the escrow purse, and debiting it from the main purse, and terminating communications;

such that the electronic cash value of the service is placed in the escrow purse for later reconciliation.

12. A method according to claim 11, wherein the request for transfer is part of a predefined series of progressive debits, and the value recorded for the transaction in the escrow purse represents the sum of the progressive debits.

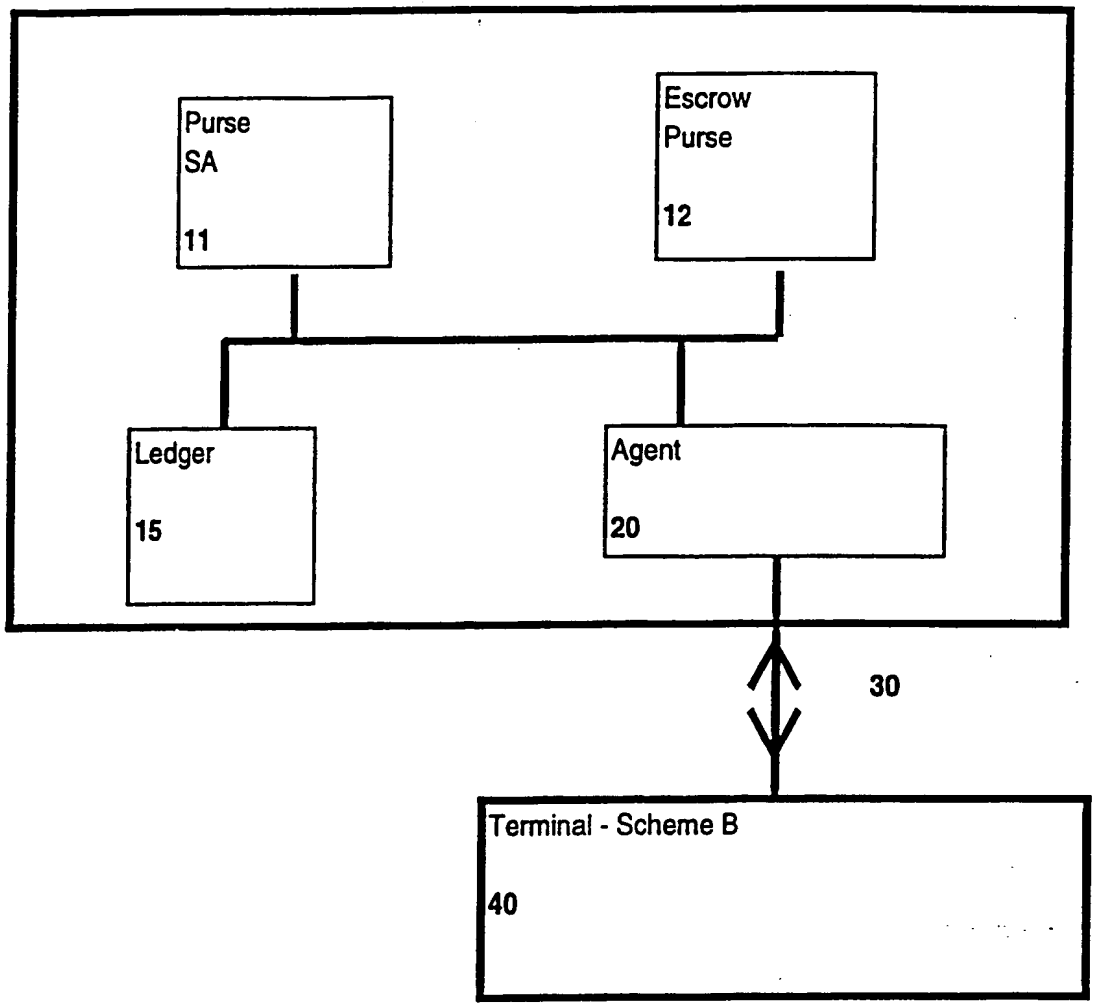

Purse
SA
11
Escrow
Purse
12
Ledger
15
Agent
20
30
Terminal - Scheme B
40

Figure 1

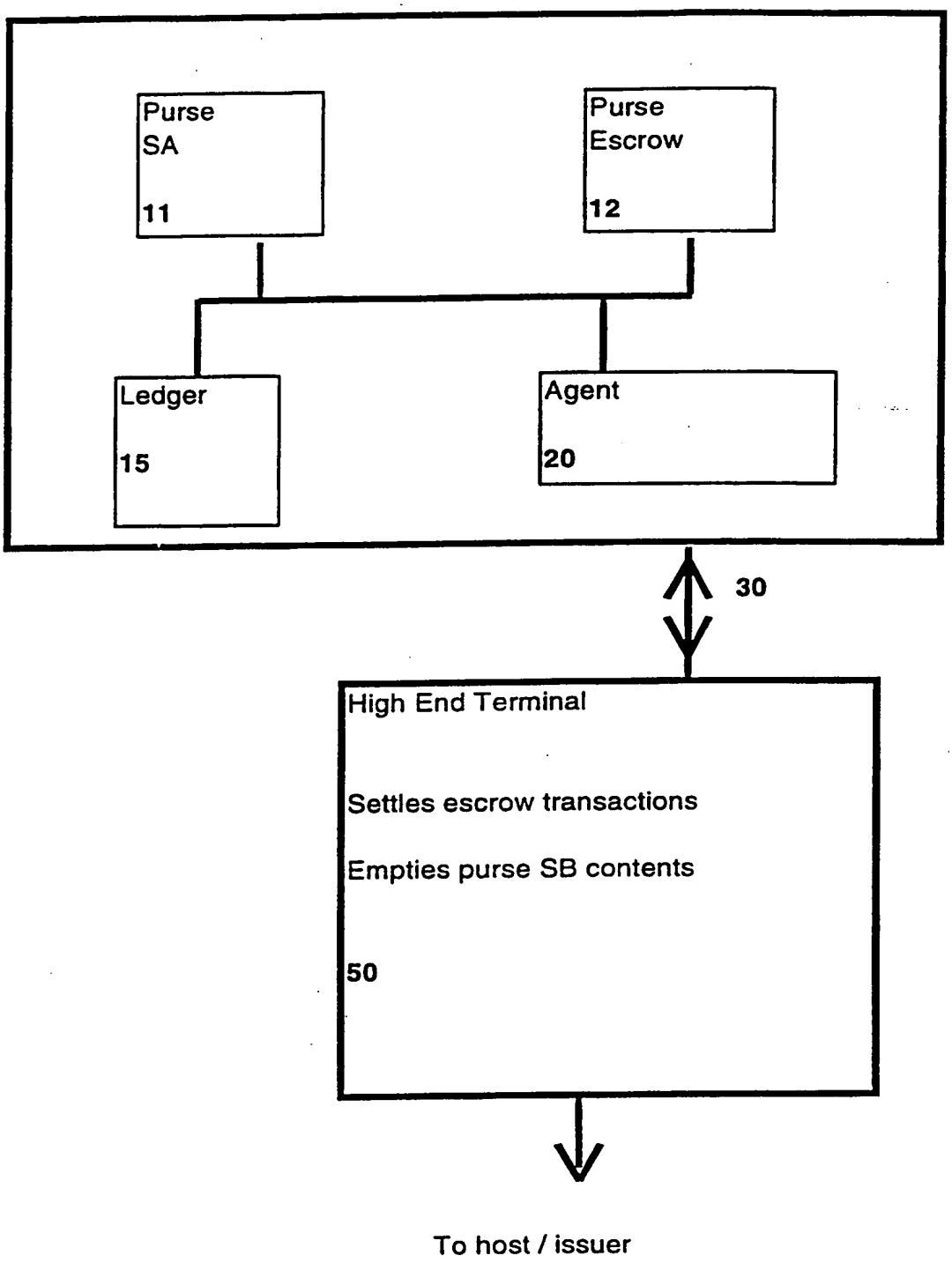


Figure 2

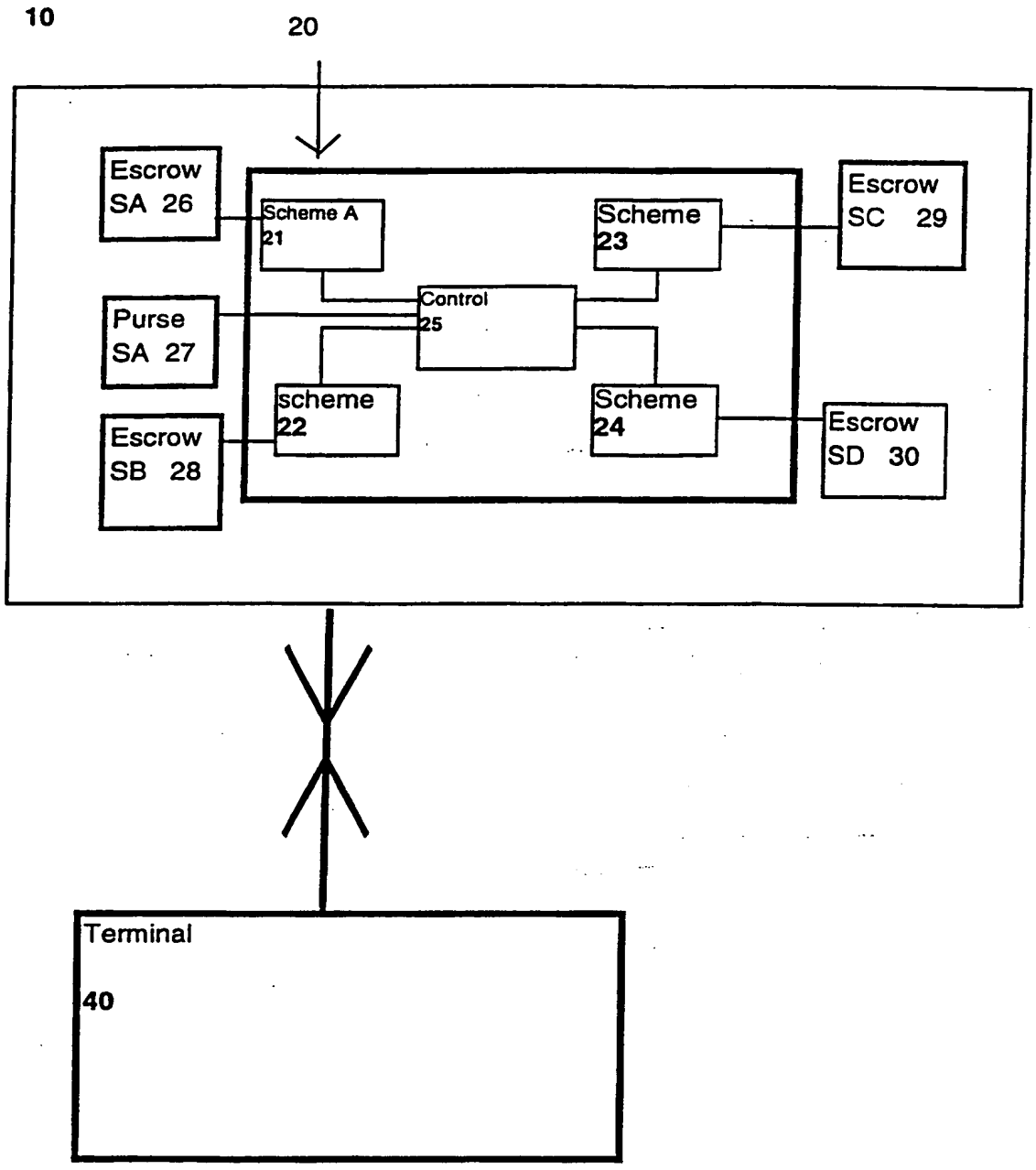


Figure 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU 99/01037

A. CLASSIFICATION OF SUBJECT MATTER

Int Cl[6]: G06K 19/067

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC: AS ABOVE AND G06K 19/07, 19/073

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
AU IPC AS ABOVE

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Derwent WPAT, USPTO
keywords: smart card, escrow, trust

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 9308545 (Jones et al.) 29 April 1993	1 to 12
X	US 5426281 (Abecassis) 20 June 1995	1, 10 , and 11

☐ Further documents are listed in the continuation of Box C

☐ See patent family annex

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
16 December 1999	21 DEC 1999
Name and mailing address of the ISA/AU	Authorized officer
AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustralia.gov.au Facsimile No. (02) 6285 3929	P. CLAYTON-STAMM Telephone No.: (02) 6283 2168